Int. j. inf. tecnol. (April 2021) 13(2):573–579
https://doi.org/10.1007/s41870-021-00611-3

ORIGINAL RESEARCH

A review of effectiveness of Saudi E-government data security management

Awad Saleh Alharbi[1] · George Halikias[2] · Muttukrishnan Rajarajan[2] · Mohammad Yamin[3]

Received: 26 November 2019 / Accepted: 4 January 2021 / Published online: 28 January 2021

Abstract Security of data has always been a contested issue since the internet became the way of life. The internet and Web 2.0 followed by Web 3.0 have enabled many applications for the use of the citizens. E-government is one of them. Questions have always been raised about the security of data in E-government applications and services. Saudi Arabia is one of the developing countries when it comes to the internet-based services. This paper attempts to review the effectiveness of security policies when dealing with threats and vulnerabilities. We shall study these aspects in the context of Saudi Arabian E-government. E-government, anywhere in the world is a very sensitive area when it comes to ensuring security of the users as well as the corporate data. Breach in security of user data may have catastrophic implications in some cases.

Keywords E-government · Security · Threats · Vulnerabilities · Saudi Arabia · Yasser · Stakeholders

✉ Awad Saleh Alharbi
awad5858@yahoo.com

George Halikias
g.halikias@city.ac.uk

Muttukrishnan Rajarajan
r.muttukrishnan@city.ac.uk

Mohammad Yamin
myamin@kau.edu.sa

[1] City, University of London, London, UK

[2] Department of Electrical and Electronic Engineering, City, University of London, London, UK

[3] Faculty of Economics and Administration, King Abdulaziz University, Jeddah, Saudi Arabia

1 Introduction

Security of data has always been a hot issue for corporations, businesses and individuals. Breach in users' data as well as that of organizations, can be devastating for citizens and government. It is the responsibility of the custodians to protect the data in their care. In this paper we shall study the details of Information Security policy of the Kingdom of Saudi Arabia in case of E-government. Our study will discuss vulnerabilities and threats posed by intruders to gain access to sensitive data or lack of safeguards in protecting the data. Privacy and security of location-based servers' data are discussed in detail by Yamin and Abi Sen [1]. Many aspects of E-government in Saudi Arabia are discussed by Basahel and Yamin [2], and Yamin and Matar [3]. Some aspects of E-government in Jordan, which falls in the same region as Saudi Arabia, are discussed in [4].

The selection, deployment and employment of sound information security controls in any E-government is crucial and often results in major implications in the assets and operations of governmental agencies in addition to the benefits of end users. Information security policy refers to the technical, operational and mechanical countermeasures or safeguards prescribed to enhance protection of availability, integrity and confidentiality of the information and the system.

It is a guide to adopt a policy to direct stakeholders to abide by the system structure to prevent such threats as unauthorized access to invasion of personal information. For instance, end users should access e government portals from safe and secure internet connections preferably using their personal computers and mobile phones instead of public computers and cyber cafes.

This article provides an overview of Saudi E-government data security and presents results of a number of

interviews conducted to assess the security aspects of these services. Our research is based on the qualitative analysis of the interviews which we had conducted on security aspects of E-government in Saudi Arabia.

2 Literature review

We shall group review of literature in different categories.

2.1 E-government

Since its introduction, the concept, service model, policies and other associated issues of E-government have been studied extensively by many researchers. E-government policies have over the years been framed by many national, regional and international organizations. For example, [5] have discussed framework for E-government including the security aspects relevant to the associated technology. Policies regarding the E-government in Saudi Arabia can be found in [6]. Various case studies of E-government of Saudi Arabia can be found in [7–10].

Concerns and safeguards to protect data have taken a much bigger stage with usage of internet. While internet is a gift to the society, its misuse by breach of data can be very harmful to individuals and the society at large. With the ongoing threats of cyber-attacks, the Saudi Arabian government has made remarkable improvements in digitization of the public sector. According to rankings by the United Nations E-government Survey 2018 (Chapter 7) [11], Riyadh stood at position 30 in the group of countries performing 50% to 75%. In 2014, for instance, the government average score stood at 0.75 EGDI scores ranking position thirty-six globally out of 193 nations surveyed. Australia was atop the survey scoring "very high" with averages scores of 0.91 closely followed by United Kingdom at 0.87. For details, refer to [12]. Several government services in Kingdom of Saudi Arabia are available online such as record online application and renewal of passports and filing of tax returns. The Saudi portal website [13] affords access to most government services under one roof. With the wide penetration of e government and commerce services in the Kingdom, enhanced adherence to privacy and security policies in all public enterprises is of high importance. In this article our focus is on the study of E-government data security in the case of Saudi Arabia.

2.2 General information about the Kingdom of Saudi Arabia

Saudi Arabia, an oil rich country, has in the twenty-first century undergone tremendous developments, modifications, pupation and changes by embracing and providing latest technologies to its citizens and businesses. Saudi Arabia represent strong cultural and religious past. Makkah (Mecca), the religious center of nearly one and a three quarters of Muslims on this planet, is the birthplace of the prophet of Islam. Saudi Arabia hosts millions of pilgrims every year for the annual and ongoing pilgrimages known as the Hajj and Umrah, which take place in and around Makkah. An estimated ten million people perform religious rituals during these pilgrimages. This pilgrimage has a great impact on the Saudi civil and civic services and in particular the services provided by the government of Saudi Arabia. The services sought for these pilgrims include grant of permission for hajj and issue of suitable visas, security clearance, travel, health and well-being management, accommodation and guidance. Thus, any policies which are used for the provision of E-government have to take these pilgrims into consideration. Many aspects of Saudi Arabia are extensively studied by many researchers including [14–20]. The most recent developments governing Saudi Arabian modernization are stipulated in the Saudi 2030 Vision [21].

3 The case of Saudi Arabia

The Saudi Arabia's Information Security policy demands that all governmental agencies in accordance to Saudi Laws contained in Executive decrees, policies, regulations, standards and orders must deploy sufficient security controls in the security requirements. Despite this, determination of appropriate mix of security controls poses the greatest challenge. The national security policy provides appropriate recommended selection of security policies mix for enhanced protection of information systems. The policy document developed in 2007 during the launch of Yesser program [22] has safeguarded the E-government structure over time. However, it has not prevented cyber-attacks altogether. The purpose of this paper is to assess the effectiveness of the Saudi Arabia's E-government system.

The Yesser program, measuring its effectiveness in preventing threats and vulnerabilities. The study further provides insights to enhance Yesser program's information security, further improve the skills of IT specialists and increase consumer uptake of the program, thereby improving the life quality of Saudi citizenry. Saudi Arabia represent strong cultural and religious past. The country is a birthplace of Muhammad (PBUH), the prophet of Islam. Saudi Arabia hosts millions of pilgrims every year for the annual and ongoing pilgrimages known as the Haj and Omrah. An estimated ten million people perform religious rituals during these pilgrimages. These pilgrims have a great impact on the Saudi civil and civic services and in particular on the E-government provisions. The services

sough for these pilgrims include grant of permission for hajj and issue of suitable visas, security clearance, travel, health and well-being management, accommodation and guidance. Thus, any policies of E-government have to take these pilgrims into consideration.

3.1 Significance of our study

The Kingdom of Saudi Arabia's E-government Security policy aims at securing data resources and uphold a tri-set of data security features, namely: data integrity, its confidentiality and availability. Information security should not appear as restrictive or preventative to daily operations but instead facilitate safety in information safety from a wide array of threats and enhance business perpetuity, minimize damage costs and maximize use of information system. Improved information security has multifold benefits. Firstly, it assuages consumers of confidentiality about the Yesser program resulting to better services and delivery. Secondly, economic development trickles following stable foundation for effective and sustainable relationship among different economic sectors. With enormous resources at their disposal, it is the prerogative of governments to provide realization of information security principals. Consequently, it is archetypical to achieve successfully information security policy in Saudi Arabia, enabling striking multiple objectives. For instance, optimization of internal government business structures with free flow of information and synchronized sharing of will set in. Sharing of personal identification numbers among government departments enhances tracking of taxpayers, offenders and credit defaulters will enhance ease of doing business, informing government of appropriate programs for different users thereby curbing social ills and improve the country's international relations. Foreign investors will trickle into the kingdom bring along additional investments from abroad and thereby strengthening Saudi Arabia's competitiveness in international investment markets.

Equally, E-government information security increases government's effectiveness and response to major social and economic problems. End user's information freely but securely shared provides the government with objective and verifiable information to adjust its policies effectively and appropriately. For instance, demographic information on college students suffering from diabetes may inform the government's ministry of health to develop advocacy and sensitization campaigns in campuses informing students on better living and lifestyle change. Equally, information on employability of graduates may inform the government through the ministry of higher education to overhaul the curriculum discourse. Consequently, information security policy is vitally beneficial to the kingdom in the long run, regionally and globally.

3.2 Research questions

This study will seek to answer the following questions with the aim of achieving the objectives of this study.

3.2.1 *How effective is the Saudi Arabia's e government security policy in safeguarding government services?*

3.2.2 *What protection safeguards does the security policy propagate in protecting the e government infrastructure?*

3.2.3 *What are the major concerns of the consumers of the e government and how can the government address them?*

3.3 Objective of our research

This study seeks to:

3.3.3 *Determine the effectiveness of the E-government's security policy in protecting provision of government services online*

3.3.4 *Identify the protection safeguards recommend in the security policy to protect the e government infrastructure*

3.3.5 *Assess the vulnerabilities and threats prevalent in the e government's security policy and how to mitigate them*

4 Saudi E-government policies and their effectiveness

As in the case of evolution of many human interactive services, E-government has emerged from the combination of internet and web 2.0. E-government is synonymous with digitization of public sector; it goes beyond digitizing the civil service. It refers to the integration of information and communication technology (ICT) in the public sector intended to enhance provision of government services, increase transparency, save costs and perpetuate the government as accessible, responsive and in touch with the public. In spite of multifold launch and deployment of E-government initiatives globally, successful E-governments are significantly few and especially in developing countries. True, organizational, ICT infrastructure, social and political factors determine the partial or success of E-government altogether. We infer from [6] that the non-technical issues directly attribute to E-government initiative failures in most developing countries.

4.1 Users' trust in security and privacy policy

Users have always been concerned about the security and privacy of their data in internet-based services. Multi studies on E-government in Saudi Arabia context hypothesized need for two types of trusts in E-government and E-commerce initiative success, namely: government trust and internet trust. An update on latest policies appears in the CITC annual report which includes details of the latest policies and governance of Saudi Arabia's digital and E-government policies and Vision 2030 [23]. For instance, it was realized that 29% of interviewed Saudis attributed online shopping with safety fears. It also revealed strong assertive relationship between adoption of E-commerce and security and privacy issues emphasis among Saudi buyers and sellers. Still, Alharbi [16] found out security and privacy issues as two important barriers to E-govern and E-commerce adoption in Kingdom of Saudi Arabia. Additional studies on KSA's E-government have revealed that users' level of trust differed across different governmental agencies subject to user experience reporting by friends, family, media and own personal experiences.

4.2 Security policy in wed design

Designing security policy for internet-based services is usually an act of government. There seems to be a general lack of information on the security aspects of e-services in general and E-government in particular in the context of Saudi Arabia. The future of web portals in Saudi Arabia should witness proper guidelines governing with the web portals.

4.3 Accountability and monitoring of governmental agencies implementing Yesser program

A number of researchers have identified issues affecting security in Yasser program. In particular, Khaled [24], in his thesis dissertation identifies multiple vulnerabilities with the Yesser program's security policy. Firstly, the program does not inculcate monitoring and accountability of governmental agencies implementing e government services in their operations. Khaled cites inadequate professionalism as a major vulnerability in implementation of the program's e government security policy. AlGarni [25] has carried out an in-depth study of the information security policy of E-Government in Saudi Arabia. He has discussed many aspects of the Yesser's provision of these services.

4.4 Decentralization and restructuring implementation of E-government security policy

Governments have always have a choice between centralized and decentralized service model as a policy regime. In instituting an E-government's security policy, a centralized entity does the heavy lifting. As a result, implementing the policy across different governmental agencies becomes a complex and intricate process. Alyabis [26] offers that restructuring policy regulations and rules and flexibility sits at the center of a more transparent, accessible and democratic government as well as safe and secure system of online transactions.

4.5 Qualified and skilled manpower

Full proof secure E-government system bedevils presence of skilled and qualifies personnel to forecast, preempt, prevent and heal security loopholes. Inadequately skilled national Saudis in IT sector harbor successful implementation of e government security policy. Foreigners and expatriates are sadly in charge of securing Yesser's infrastructure. Nonetheless, revamped scholarships, trainings and academicians in the IT field in the past decade will seal this vulnerability in the near future.

From a number of studies that we have mentioned, we find growing evidence that Yesser's implementation requires above average internet users in Saudi Arabia. Over the years, internet connectivity, penetration and Yesser adoption remains at between 50 and 55 per cent of the population. The Computer Emergency Response Team proactively and reactively sensitizes and assuages Yesser program users of safety, privacy, reliability and security. In addition, its services cover both public and private enterprises using the Yesser program's infrastructure.

5 Our study

We have conducted seventeen interviews of stakeholders of E-government services in 2019. Here we provide qualitative analysis of the interviews that we have conducted for the purpose.

5.1 Qualitative analysis

We designed 10 questions for the interviews of a selected group of Saudi E-government users. A list of these questions is available in Table 1. It is evident from this list that the qualitative analysis was suitable for our purpose. We compiled a list of users for the interviews which represented different age groups of both male and females from Qasim and Makkah regions of Saudi Arabia. We took all

Table 1 Questionnaire for qualitative analysis

1	What are your views about the quality of Saudi E-government applications
2	What are your views about the quality of Saudi E-government portal
3	Data and information in the application about services serves its intended purpose
4	What are your views about the frequency of downtime of services
5	What are your views on the need for security of data in applications
6	Are there any concerns on security of data in these applications
7	What are your views on Yasser's program and its provision of security mechanisms
8	In which areas the security can be enhanced
9	What should be done to improve the data security in applications
10	Is there a need to audit the Yasser's security mechanisms

the standard precautions of the privacy and security of the respondents. These people were asked to respond to our questions on different aspects of data security of Saudi E-government as can be seen from Table 1. In some cases the responses were short while the others were detailed. In the next section we present an analysis of the responses followed by conclusions.

5.2 Analysis of the responses

The qualitative analysis of the questionnaire is based on seventeen interviews of the respondents who had previously used Saudi E-government and possessed good knowledge of the topic and service.

When asked about the quality of the E-government applications as in Question 1 (Q1), twelve respondents were found to be satisfied with overall quality of the applications, three were somewhat satisfied and two were unhappy. As for the quality of the E-government portal, as in Q2, fourteen respondents affirmed satisfaction with the overall features of Saudi E-government portal, two were neutral while one was unhappy. Double security verification features including sending a code to one's phone number were appreciated as important security features. The interviewees appreciated the colorful and eye catching graphic features on the portal.

For Q3, thirteen respondents expressed satisfaction with the usefulness and relevance of data and information in the application about services in serving the intended purpose, three expressed somewhat satisfied while one was unsatisfied. User's demographical details such as age, sex, and marital status, and occupation, date of birth and level of education were particularly considered as relevant and useful among interviewed stakeholders.

For Q4, sixteen respondents confirmed their satisfaction with the E-government user experience. The basis for their affirmation mainly rested on the fact that the service was quite stable with the downtime frequency of the service converging to zero. One respondent, however, expressed unhappiness due to slow internet connection accessed over a smart phone in a remote location. However, none of the respondents expressed dissatisfaction with E-government services over high frequency of downtime.

For Q5, twelve respondents were found to be satisfied with overall level of security of the e government service, two were somewhat satisfied and three were unhappy. Fourteen respondents did not have any concerns on overall security of the service and three of them were somewhat satisfied. None was unhappy. The three cited data and site encryption as an added security feature missing in the e government portal. For Q7, fourteen respondents were satisfied with the Yasser's program and its provision of security mechanisms, two were somewhat satisfied while one was not satisfied. All of the fourteen respondents were satisfied with the programs security features and did not propose any areas for security enhancement. However any future improvements were welcome by all the respondents. There were some suggestions made by some of the interviewees. Two of them suggested that the login should be restricted to only within the country to enable monitoring the IP addresses that breach data. These respondent felt that perpetual monitoring of the Yasser's program and transparent reporting of any breaches will further enhance security features. For Q9, fifteen respondents did not propose improvement in data security of e government applications saying they were satisfied while two were somewhat not satisfied. They recommended data encryption as an important security improvement. Finally, for Q10, fourteen of the respondents affirmed their support for need to audit the Yasser's security mechanisms; two were satisfied with the present state while one was dissatisfied with the audit frequency and coverage.

5.3 Analysis and discussion of results of the responses

From the analysis of survey responses of the subsection 5.2, it is clear that a convincing majority of respondents have backed the initiatives of the Saudi Arabian government in providing and tightening privacy and security

mechanisms related to E-government Applications data. Although majority of responses are in general appreciative about Yasser's program and mechanisms but in the same time they have expressed their opinion to audit are the program on a regular basis. We expected some suggestions from the respondents to improve the security mechanisms but we didn't get any. Instead, the respondents expressed their full satisfaction. In general, 85% or more respondents were satisfied with the overall security program and their huddling by the government. In a few cases, there were two or three respondents who were not entirely satisfied but they didn't provide any suggestions to improve the program.

6 Conclusions

Data security and privacy in the E-government applications are major issues. In particular, there usually are sensitivities with the user data, which should never be compromised. Therefore, it is the duty of the E-government providers to ensure that the user data is kept secure and safe. In the case of Saudi Arabia, from the analysis and foregoing discussion, it is clear that the Saudi government has made serious efforts and have done a good job in the shorter than usual time to improve the security of data and its management. However, there are still some areas where data security requires improved management. It is the responsibility of government organizations, corporations and business organizations to take advantage of the Saudi government's liberal policies to provide help in setting up infrastructure. The government has already provided the nation with state of art internet facilities. Fiber Optics internet technology, with its fast speed, which Saudi organizations are enjoying, should help even further to improve the security of data involved in E-government. In particular it is suggested that Yasser program should undergo a security audit to ensure the highest level of the privacy and safety. This will boost the confidence of the users and all hesitations will be eradicated from the minds of the people. It must be born in mind that the personal privacy is even more critical and difficult to provide and maintain in the E-government services, especially in the associated web portals.

References

1. Yamin M, Abi Sen AA (2018) Improving privacy and security of user data in location based services. Int J Ambient Comput Intell (IJACI) 9(1):1
2. Basahel A, Yamin M (2017) Measuring success of E-government of Saudi Arabia. Int J Inf Tecnol. https://doi.org/10.1007/s41870-017-0029-4
3. Yamin M, Matar R (2016) E-government Saudi Arabia—an empirical study. BIJIT BVICAM's Int J Inf Technol 8(1):944–949
4. Al-Shboul M, Rababah O, Al-Shboul M, Ghnemat R, Al-Saqqa S (2014) Challenges and factors affecting the implementation of E-government in Jordan. J Softw Eng Appl 7:1111–1127. https://doi.org/10.4236/jsea.2014.713098
5. UN E-Government knowledgebase. Online. 2019. https://publicadministration.un.org/egovkb/en-us/About/UNeGovDD-Framework. Accessed date 11 Nov 2019
6. Saudi National Portal (About eGovernment). [Online]. 2019.https://www.saudi.gov.sa/wps/portal/snp/pages/egovernment. Accessed date 11 Nov 2019
7. Basahel A, Yamin M (2017) Measuring success of E-government of Saudi Arabia. Int J Inf Technol 9(4):1. https://doi.org/10.1007/s41870-017-0029-4
8. Alssbaiheen A, Love S (2015) m-Government adoption in Saudi Arabia: challenges and opportunities. Int J Technol Hum Interact (IJTHI). https://doi.org/10.4018/ijthi.2015070104
9. Ullah Khan H, Alsahli A, Alsabri H (2013) E-government in Saudi Arabia: analysis on present and future. J Electr Commun Eng Res 1(3):2321–5941
10. Yamin M, Mattar R (2016) E-government Saudi Arabia—an empirical study. BIJIT BVICAM's Int J Inf Technol 8(1):944–949
11. United Nations E-Government Survey: (Gearing E-government to support transformation towards sustainable and resilient societies 2018. Chapter 7. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018%20Preliminary%20pages.pdf. Accessed date 11 Nov 2019
12. Alharbi AS (2016) The Future of E-government in Saudi Arabia. Int Multiling Acad J. http://aasrc.org/aasrj/index.php/imaj/article/view/1812. Accessed date 24 Nov 2017
13. About Unified National Platform GOV.SA. [Online]. Accessed date 11 Nov 2019 https://www.my.gov.sa/wps/portal/snp/aboutPortal/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zivQIsTAwdDQz9_d29TAwCnQ1DjUy9wgwMLEz1w9EUGJs6ARX4mvs7BocZGhiY6kcRo98AB3A0IKw_Ck0JpgvACvBYUZAbGmGQ6agIAFnInkA!/dz/d5/L0lDUmlTUSEhL3dHa0FKRnNBLzROV3FpQSEhL2Vu/
14. Yamin M (2018) Managing crowds with technology: cases of Hajj and Kumbh Mela. Int J Inf Technol. https://doi.org/10.1007/s41870-018-0266-1.(Springer)
15. Basahel A, Yamin M, Drijan A (2016) Barriers to cloud computing adoption for SMEs in Saudi Arabia. BIJIT BVICAM's Int J Inf Technol 8(02):1044–1048
16. Yamin M, Al Amri SA (2016) Mobile applications and customers satisfaction in Saudi electricity company. Int Multiling Acad J 3(2):66–81
17. Yamin M, Al Harbi O (2016) Online shopping adoption in Saudi Arabia: an empirical research. Int Multiling Acad J 3(2):1

18. Yamin M, Aljihani S (2016) E-learning and women in Saudi Arabia: an empirical study. BIJIT BVICAM's Int J Inf Technol 8(1):950–954
19. Mohammad Y, Moteb A (2014) An architecture for Hajj management, 15th IFIP WG 8.1. Proceedings international conference on informatics and semiotics in organisations, ICISO 2014, Shanghai, China, May 23–24, 2014, IFIP advances in information and communication technology. Vol. 426
20. Mohammad Y, Ades Y (2009) Crowd management with RFID and wireless technologies, proceedings of first international conference on networks and communications. IEEE Comput Soc Washington, DC, USA
21. Vision 2030 (Saudi). https://vision2030.gov.sa/en. Accessed date 11 Nov 2019
22. Yesser E-government Program, Online.2019. http://www.yesser.gov.sa/EN/mediacenter/Annual_Reports/Anual%20Report%20foe%20web.pdf. Accessed DATE 11 Nov 2019
23. CITC Annual Report (A Saudi web portal). Online. https://www.citc.gov.sa/en/MediaCenter/Annualreport/Pages/default.aspx. Accessed date 11 Nov 2019
24. Khaled J (2015) The e-government in the Kingdom of Saudi Arabia: the perceptions, trust levels and concerns among the Internet users (Master's thesis, Griffith University, Brisbane, Australia, 2016). Int J Comput Sci Inf Technol 5(6):6892–6901
25. Khaled A (2015) Information security policy for E-government in Saudi Arabia: effectiveness, vulnerabilities and threats. Thesis. Rochester Institute of Technology. Accessed from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=9788&context=theses
26. Alyabis FA (2000) Examining the impact of Internet electronic commerce on commercial organizations in Saudi Arabia—scholarworks.uni.edu. Online. https://scholarworks.uni.edu/etd/741/. Accessed date 11 Nov 2019